Computer Communications 31 (2008) 3405–3409

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A WEP post-processing algorithm for a Robust 802.11 WLAN implementation

Taskin Kocak [a,*], Mohit Jagetia [b]

[a] Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, UK
[b] Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816, USA

ARTICLE INFO

Article history:
Received 16 March 2007
Received in revised form 23 May 2008
Accepted 26 May 2008
Available online 3 June 2008

Keywords:
Wireless LAN
802.11
Security
WEP

ABSTRACT

Wired Equivalent Privacy (WEP) protocol used within the IEEE 802.11 standard has "major security flaws" thus wireless local area networks (WLANs) using the protocol are vulnerable to attacks. In this paper, we propose a scrambling algorithm that reduces the security vulnerabilities of the WEP. The algorithm randomizes the data and prevents access from unauthorized users by adding some standard randomness to it. This random characteristic is a function of the private attribute shared between transmitter and receiver only. In this approach the randomness is achieved by RC4 algorithm, and the distribution of the randomness is provided with different algorithms to increase the complexity of rectifying the encrypted data and optimize utilization of the randomness. The algorithm is developed with a consideration for the least computational requirements to achieve both power and cost efficiency. The proposed software solution takes the WEP output as input and the original WEP implementation is not touched, thus it is an easy patch for the deployed systems.

1. Introduction

Internet enabled wireless devices continue to proliferate and are expected to surpass traditional wired Internet clients in the near future. The use of wireless networking is rapidly rising with an ever-increasing need for businesses to cut costs and provide mobility to workers. Wireless technology has spread to devices from small-embedded systems to large general purpose PCs. This is due to cheaper prices, faster speeds and also due to the need for greater mobility. However, data security and privacy remain major concerns in the current generation of wireless networks. Wireless network security is very essential as it is not bound to any region. Any unauthorized person can read, modify or use the private data being transmitted over a network. As wireless platforms mature, grow in popularity, and store valuable information, hackers are stepping up their attacks on wireless targets. Thus, wireless security has become an important area of research and development. As in the wired world, wireless security boils down to protecting information and preventing unauthorized system access. However, it is challenging to implement security in small-footprint devices with low processing power and small memory capacities. IEEE 802.11 Wireless Fidelity (Wi-Fi) standard based systems are ubiquitously available. The standard refers to a family of specifications developed for wireless local area network (LAN) technology [1]. It specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The need for the 802.11 standard came due to the emergence of various proprietary wireless systems, which were incapable of interoperation. The standard has become popular due to its high data rate and its fast and easy encryption techniques. It is modeled on the ISO's OSI Model but the standard is only concerned with the physical layer and the lower part of the data link layer (i.e., the Medium Access Control (MAC) sub-layer [2,3]). The 802.11 architecture uses fixed network access points (APs) with which mobile nodes can communicate. These network APs are sometimes connected to landlines to widen the LAN's capability by bridging wireless nodes to other wired nodes. The Wi-Fi standard is designed to provide a wireless LAN with a level of security and privacy comparable to what is usually expected of a wired LAN, using Wired Equivalent Privacy (WEP) security protocol [1]. WEP is a popular wireless secure communications stream cipher protocol. It allows users to communicate with other users sharing the public key over a network. It provides authentication and encrypted communications over unsecured channels. However, several studies have demonstrated that WEP is vulnerable to various attacks and it fails to achieve its security goals [4–6,13,15,18]. The serious security flaws that have been discovered in the protocol stem from misapplication of the cryptographic primitives. The so-called WEP attacks appear in the form of intercepting and modifying the transmissions, and gaining access to restricted networks. In this paper, we propose an algorithm to patch the WEP protocol against these attacks. The developed algorithm requires a minimal solution for the various attacks in the WEP protocol. It offers guidelines to develop a practical and a viable infrastructure for robust 802.11 implementation. The proposed solution can be easily deployed

* Corresponding author. Tel.: +44 117 954 5197.
E-mail addresses: t.kocak@bristol.ac.uk (T. Kocak), mohit@cs.ucf.edu (M. Jagetia).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.05.021

Table 1
Nomenclature

BAB	Bit addressable memory bank
$Bank_j$	Memory bank j
$Cntr_j$	Counter j
C_P	Chunk position
C_S	Chunk size
field_length	Length of the IV or ICV fields
i	Number of RC4 octets used per frame
ICV	Integrity check value
IV	Initialization vector
k	Key sequence
MAC	Medium access control
MIB	Management information base
MPDU	MAC protocol data unit
n	Number of bytes in WEP cipher-text
PRNG	Pseudo random number generator
R_O	Total number of random octets
SA	Scrambling algorithm
SF	Scrambling flag

within the WEP-capable equipments. This can be done by upgrading the software in the existing systems.

The rest of the paper is organized as follows: An overview of WEP is given in Section 2; the proposed scrambling algorithm is introduced in Section 3; analysis of the proposed algorithm is presented in Section 4; the paper ends with some conclusions and directions for future work in Section 5.

Table 1 summarizes the nomenclature that is used in the remainder of the paper.

2. Wired Equivalent Privacy (WEP)

WEP is a security protocol defined in the IEEE 802.11 Wi-Fi standard. The goal of WEP is to provide the same level of security as a wired Ethernet. In IEEE 802.11 standard shared key authentication supports authentication of a station. It accomplishes this without the need to transmit the secret key in the open; however, it does require the use of the WEP privacy mechanism. Therefore, this authentication scheme is only available if the WEP option is implemented. The required secret, shared key is presumed to have been delivered to participating stations via a secure channel that is independent of IEEE 802.11. This shared key is contained in a write-only Management Information Base (MIB) attribute via the MAC management path so that the key value remains internal to the MAC. During the shared key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the pseudo-random number sequence for the key/IV pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames.

The WEP is considered to be a symmetric algorithm since the same key is used for encipherment and decipherment. A pseudo random number generator (PRNG) produces key sequence, k, using the input seed, which is formed through concatenation of the secret key and the initialization vector (IV) (see Fig. 1). The length of the pseudo random octets are equal to the number of data octets that are to be transmitted in the data plus the integrity check value (ICV). The ICV is obtained by an integrity algorithm, which uses the plaintext as input. Then, the key sequence is combined with the plaintext concatenated with the ICV to form the ciphertext. Finally, the IV is added to the ciphertext to obtain the message. The WEP PRNG is the critical component of this process, since it transforms a relatively short secret key into an arbitrarily long key sequence. This greatly simplifies the task of key distribution, as only the secret key needs to be communicated between stations. The IV extends the useful lifetime of the secret key and provides the self-synchronous property of the algorithm. The secret key remains constant while the IV changes periodically. Each new IV results in a new seed and key sequence, thus there is a one-to-one correspondence between the IV and k. The IV may be changed as frequently as every MAC protocol data unit (MPDU) and, since it travels with the message, the receiver will always be able to decipher any message. The IV is transmitted in the clear since it does not provide an attacker with any information about the secret key, and since its value must be known by the recipient in order to perform the decryption. The WEP algorithm is applied to the frame body of an MPDU. The IV, cipher-text, ICV triplet forms the actual data to be sent in the data frame.

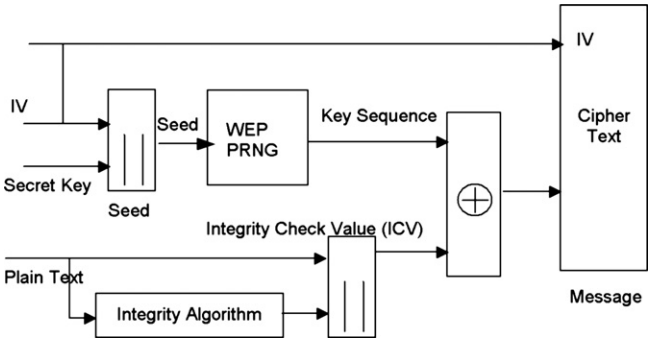

Fig. 1. WEP block diagram.

2.1. Security issues in WEP

WEP uses RC4 encryption algorithm [7], which operates by expanding a short key into an infinite pseudo-random key stream. If an attacker flips a bit in the cipher text, then upon decryption, the corresponding bit in the plaintext will be flipped. If an eavesdropper intercepts two cipher texts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts. The statistical attacks become increasingly practical as more cipher text that use the same key stream become known. Once one of the plaintexts become known, it is trivial to recover all of the others. To ensure that a packet has not been modified, WEP uses an ICV field in the packet. To avoid encrypting two ciphertexts with the same key stream, an IV is used to augment the shared key and produce a different RC4 key for each packet. The major attacks [4–6,8] to WEP are given as follows:

- *Active attack:* Modification of the packet by modifying the ICV.
- *Passive attacks:*
  - Integrity violation by analyzing the IV.
  - Table based attack for decrypting every packet that is sent over the wireless link.

In order to avoid these attacks, a novel scrambling algorithm is proposed in this work. The algorithm randomizes the data and prevents access from unauthorized users by adding some standard randomness to it. This random characteristic is a function of the private attribute shared between transmitter and receiver only. In this approach the randomness is achieved by RC4 algorithm, and the distribution of the randomness is provided with different algorithms to increase the complexity of rectifying the encrypted data and optimize utilization of the randomness.

3. The novel scrambling algorithm

There are several recently reported fixes for WEP [5,17], however many of them cannot be deployed right away due to their in-